



Protect what you value.

# You Cannot Manage, What you Cannot Measure:

## Security Risk Metrics

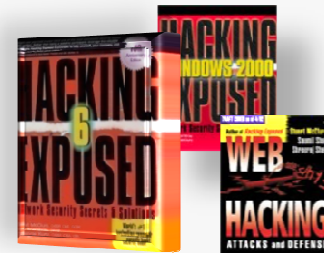
*State of CA CISO Lecture Series*

Stuart McClure  
VP Operations/Strategy  
Risk and Compliance Business Unit  
McAfee, Inc.

# Introductions

*Curriculum Vitae*

**McAfee**



# How to motivate change...

*Carrot? Stick? ...Both?*

**McAfee**

1. **Attack** (worm, malware, privacy breach)
2. **Compliance Deadlines** (FISMA, IAVA, PCI)
3. **Live Demonstrations** (approved on your own systems, databases, accounts of course!)
4. **Security Metrics** (Quantify and track your risk over time. Predict your next attack/breach...)



**In the end... It's all about relationships,  
building trust and credibility...**

# Agenda



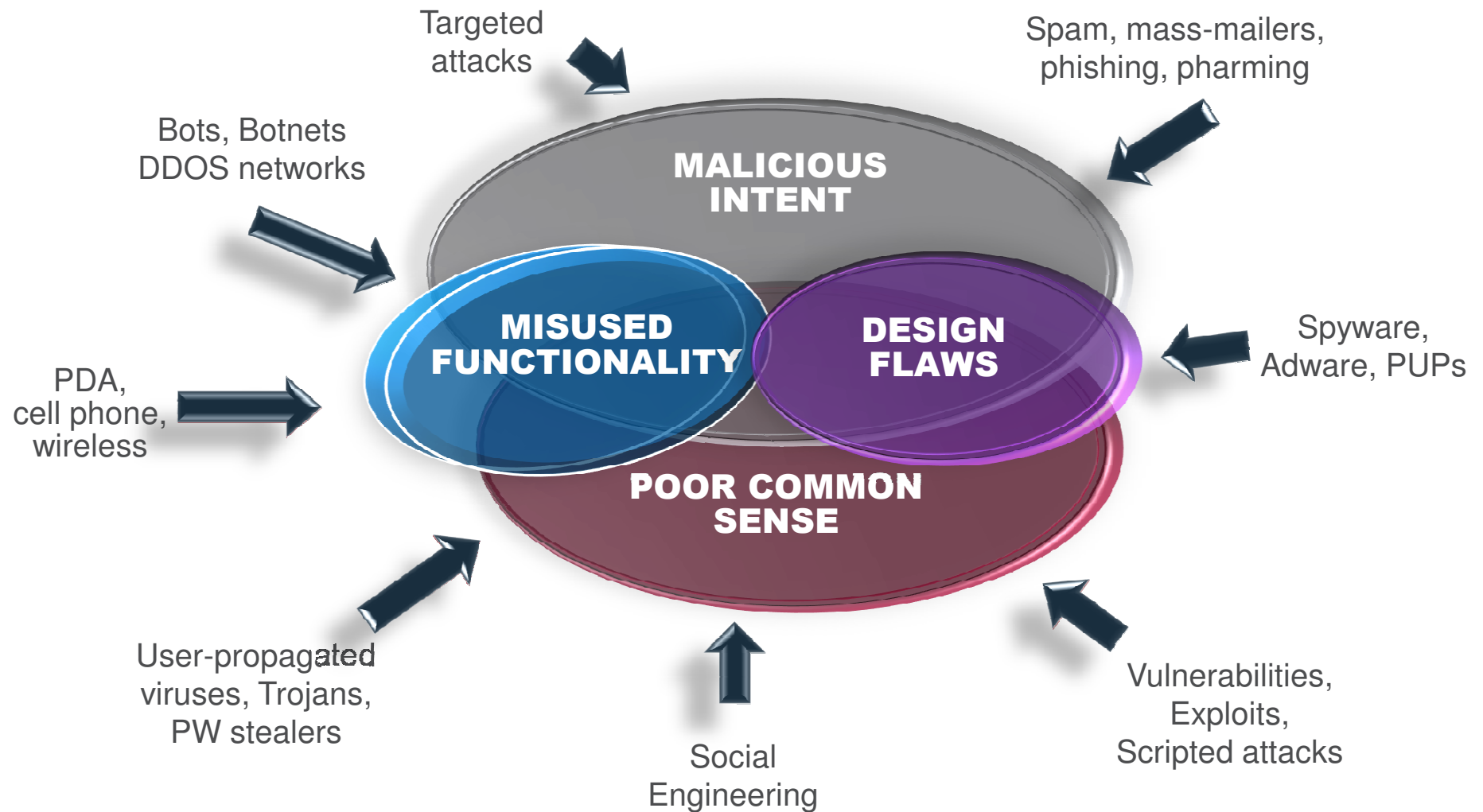
- Security Drivers
- Security Metrics
- Real World Examples

# Security Drivers

# What drives us?

*Threats: Opportunity Meets Motivation Meets Ability...*

**McAfee**





# Misused Functionality – In the Real World...

**McAfee**

- April 19, 1995
- 168 souls
- Commonly used materials costing \$5,000



# Misused Functionality – In the Security World...

McAfee

## • Famous examples:

- Mass mailing functions
  - Melissa virus (1999)
  - ILOVEYOU (2000)
- ActiveX functions
  - Zlob Trojan (2005)
- Icon modification functions
  - OSX/Leap (2006)
- Autorun/Autoplay functions
  - W32/Virut (2003)
  - W32/Sality (2006)
  - Autorun.worm.gen (2008)



- IE's Browser Helper Objects (BHO)



- PWS.Cashgrabber (2005)
- PWS.Banker (2008)
- File sharing
  - Conficker.B (2009)



*Mitre recently added new category – Common Configuration Enumeration (CCE)*

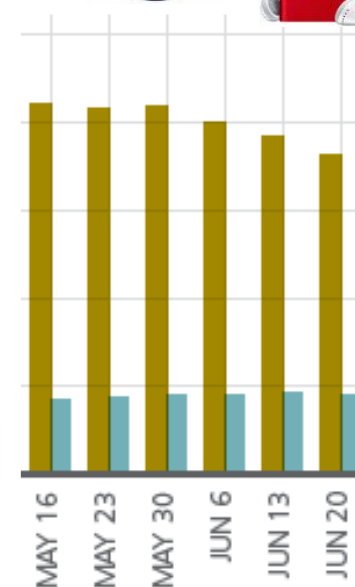
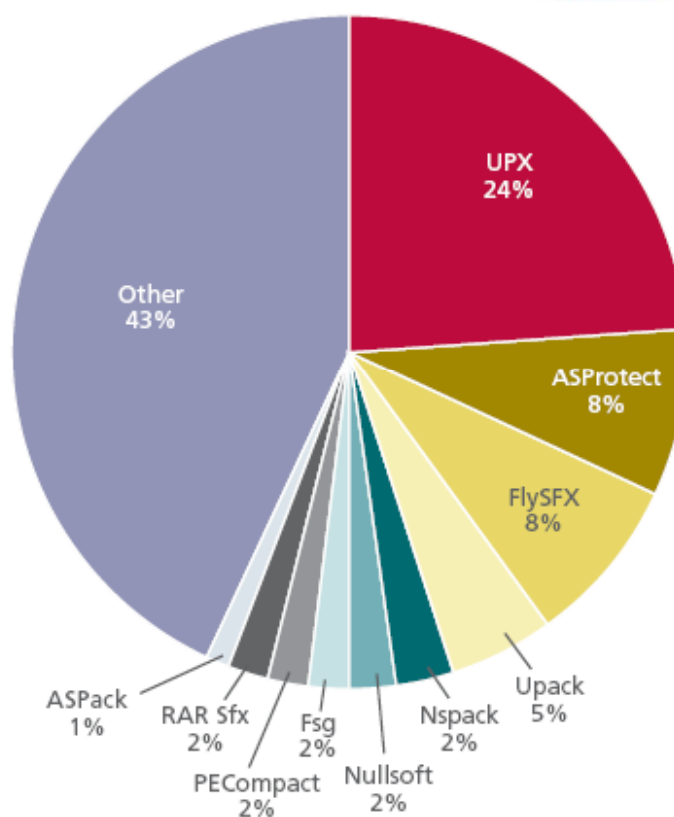
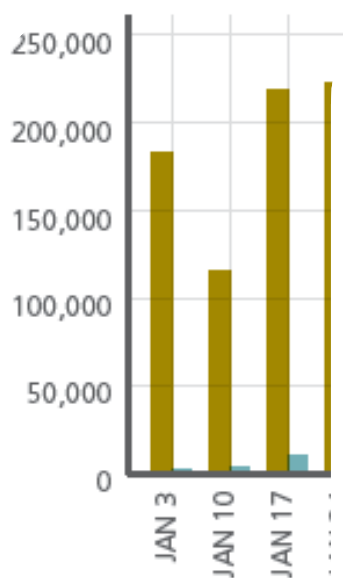




# Misused Functionality – In the Security World...

## *Autorun: The Floppy Disk of the New Millennium*

**McAfee**



# Design Flaws – In the Real World...

**McAfee**

- Feb. 24, 1989
- 9 souls
- Faulty cargo door design
- Went unfixed for years



# Design Flaws – In the Security World...



- **Famous examples:**

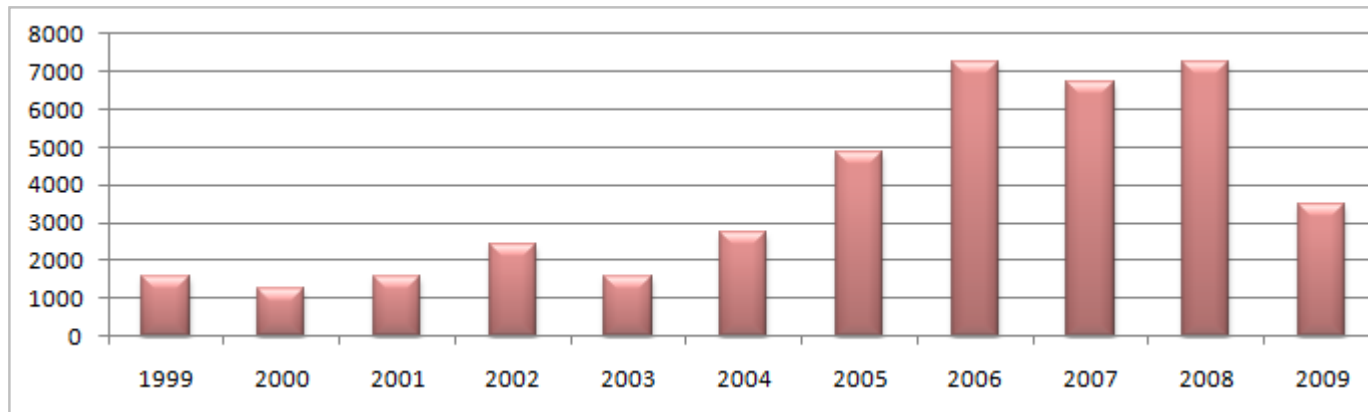
- MS01-033 (Code Red) – 2001 (1 mo)
- MS02-039 (SQL Slammer) – 2003 (6 mos)
- MS08-067 (Conficker) – 2008 (2 weeks)

- SANS reports 60% of attacks today are web based



- CVE rate = 18/day, 3700 average/yr

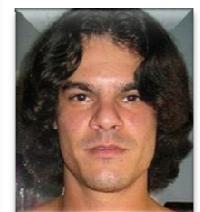
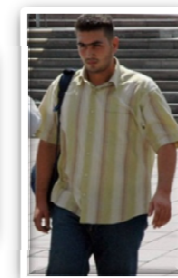
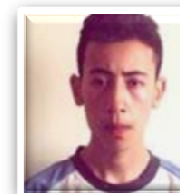
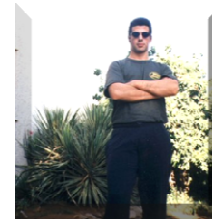
- Over 39,000 vulns in NVD. Over 40,000 in CVE:



# Malicious Intent

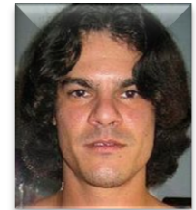
McAfee

- War Games movie (1983) [Matthew Broderick]
- *Morris Worm*\* (1988) [Robert Morris]
- Moonlight Maze (1998-99)
- “Good Times” virus (1994)
- First Word Macro viruses (1995)
- Solar Sunrise (1998) [Ehud Tenenbaum]
- *Melissa virus* (1999) [David L. Smith]
- US Military attack (2000) [Gary McKinnon]
- *ILOVEYOU virus* [Reomel Lamoires], DDOS attacks (2000)
- *Klez*\*, *Sadmind*, *Code Red*, *Nimda* worms (2001)
- *Slapper*, *Spida*\*, *Bugbear*, *Opaserv*\* worms (2002)
- Root server DoS (2002)
- *Blaster* [Jeffrey Parson], SQL Slammer worms (2003), Titan Rain (2003-2005)
- MyDoom, Witty, *Sasser/Netsky*, Korgo worms (2004) [Sven Jaschan]
- Rbot/Sdbot/Zotob (2005) [Farid Essebar aka “Diabl0” and Atilla Ekici aka “Coder”]
- *Storm Worm* (2007)
- TJX/Heartland/Hannaford, etc. (2009) [Albert Gonzalez]



## Making it Real – Recent News...

McAfee



- Three hackers indicted in NJ on 8/17/09

- 1 co-conspirator not indicted

- Allegedly responsible for:

- T.J. Maxx (94M), Heartland (130M), Home Depot (100M), 7-Eleven, Barnes & Noble, BJ's Wholesale Club, Boston (100M), Forever 21 (99k), Office Max (200k), Sports Authority

- Attacked from systems in:

- US (NJ/CA/IL), Netherlands, Latvia

- Techniques used:

- SQL Injection attacks
  - Installed malware (including AV bypassing)

- References:

- <http://www.washingtonpost.com/wp-dyn/content/article/2009/08/17/AR2009081701915.html>
  - <http://voices.washingtonpost.com/securityfix/heartlandIndictment.pdf>

**Pled Guilty**

UNITED STATES DISTRICT COURT  
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA :  
: Hon.  
: :  
v. : Criminal No. 09-  
: 18 U.S.C. §§ 371 and 1349  
: :  
ALBERT GONZALEZ, :  
a/k/a "segvec," :  
a/k/a "sounpazi," :  
a/k/a "j4guar17," :  
HACKER 1, and :  
HACKER 2 :

**INDICTMENT**

The Grand Jury in and for the District of New Jersey,  
sitting at Newark, charges:

**COUNT 1**  
(Conspiracy)  
**18 U.S.C. § 371**

1. At various times relevant to this Indictment:

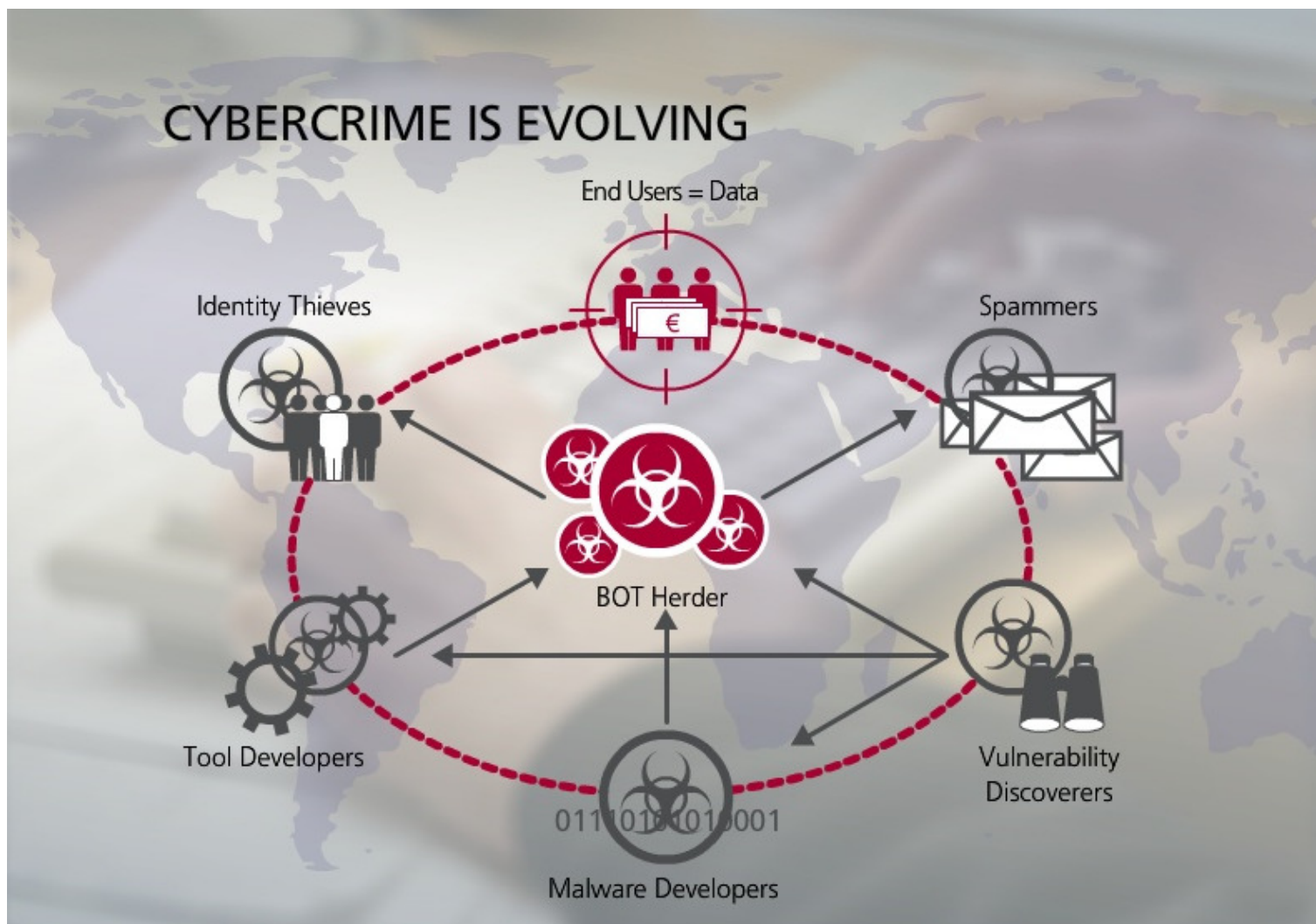
**The Defendants**

a. Defendant Albert Gonzalez, a/k/a "segvec," a/k/a



# Cyber Crime Ecosystem (The Bad Guys)

McAfee®

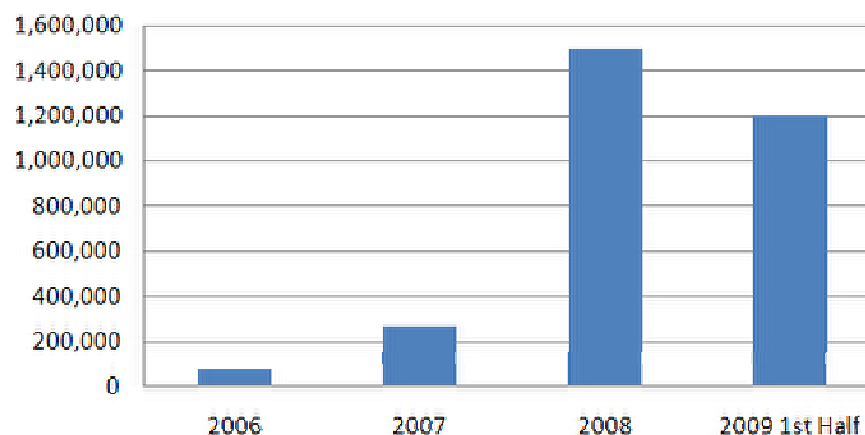




# Malicious Intent: The result - Malware YTD

**McAfee**

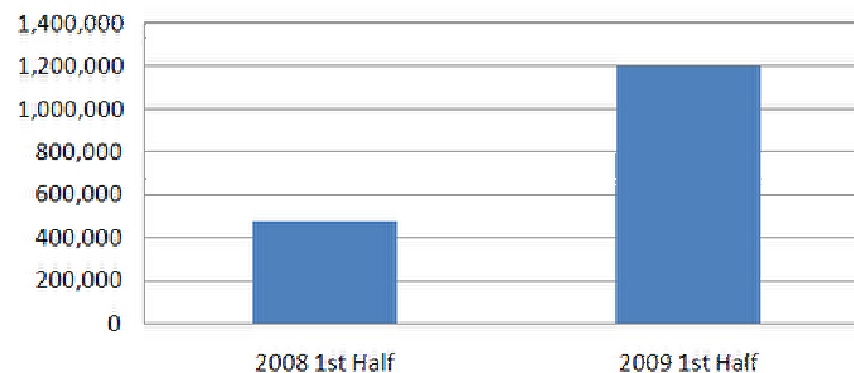
## Unique Malware Growth



- 200,000 unique malware per month
- 6,000 per day

- More than double last year's midyear metric

## Half Year Malware Growth Comparison

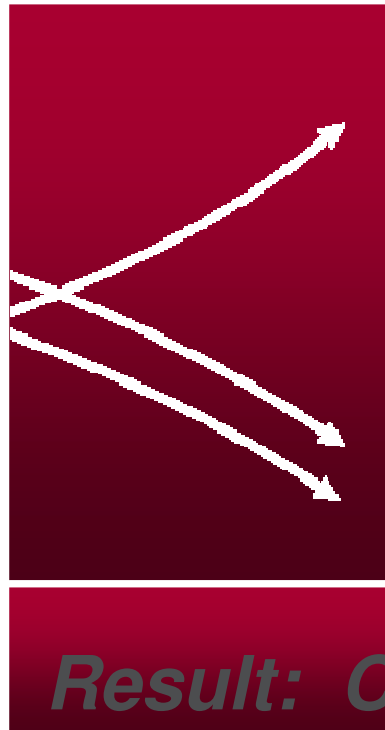


# Security Metrics

# Risk and Compliance

## *The Dilemma*

**McAfee**



### ***Increasing Risk***

Threats  
Vulnerabilities  
Change  
Regulations

### ***Decreasing Protection***

Insufficient budget  
Limited people resources

## ***Result: Controlled Chaos***

- Lost data / Privacy breaches
- Decreased system availability
- Poor system performance
- Configuration creep
- Audit/Remediate/Repeat
- Reactive fire-fighting
- Delays in strategic projects
- Lost business

## **Risk and Compliance**

### ***The Goal***

**McAfee**

1. Reduce time and cost associated with patching and audits
2. Manage more effectively against policies
3. Report-on-demand for internal or external audits
4. Increase security of my data, applications, and network
5. Enhance system availability and application performance

***Get in Control, Stay in Control***

# Risk and Compliance

**McAfee**

**Assess  
Completely**

**Remediate  
Easily**

**Enforce  
Automatically**

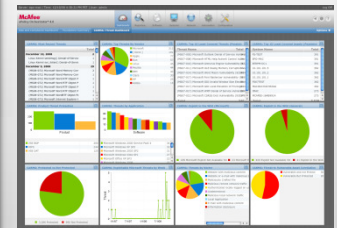
**Optimize  
Security**

**Report  
Intelligently**

***Get in Control***



***Stay in Control***



***“Audit Once, Report Many”***

Increased security and compliance

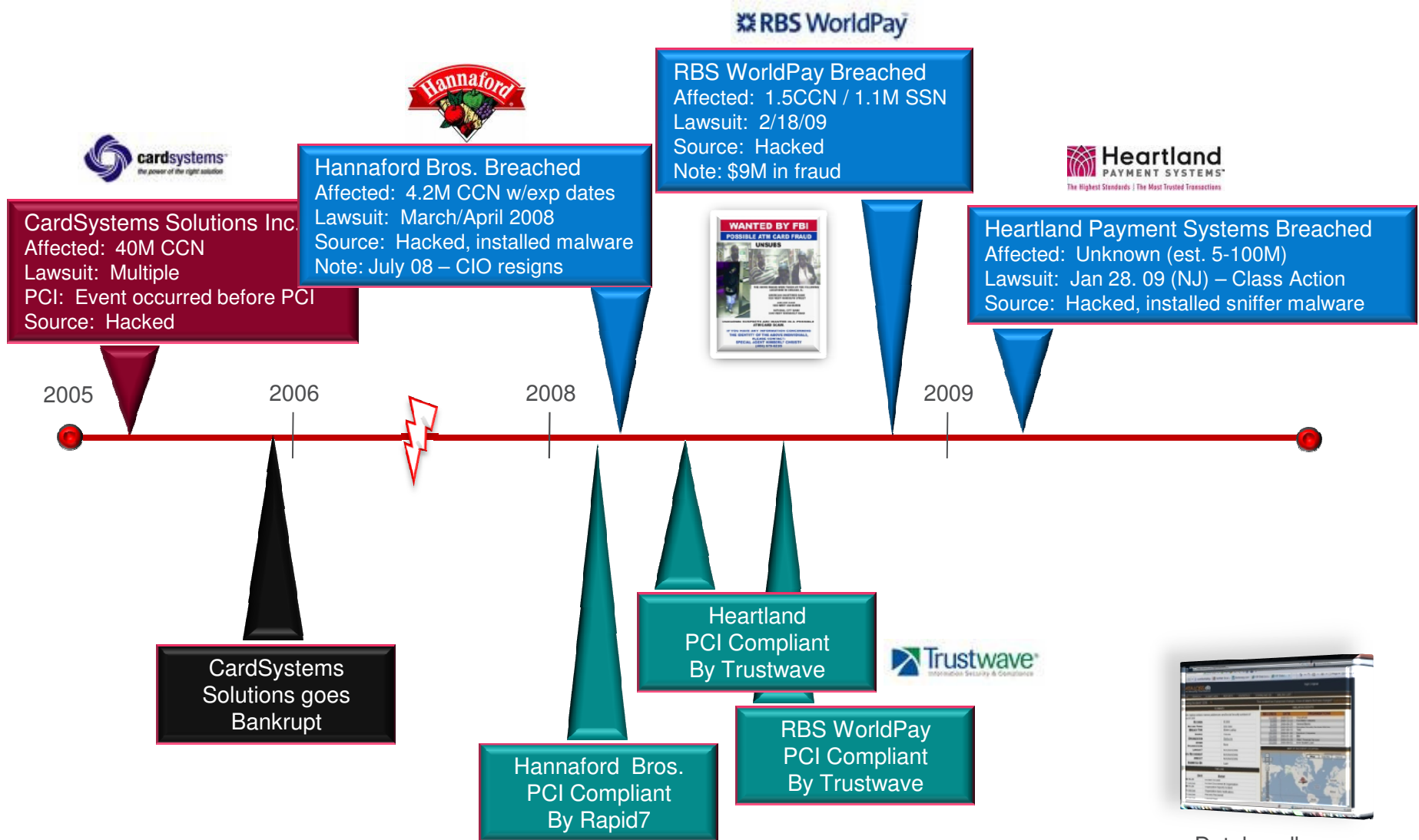
Enhanced availability and system performance

Reduced time & cost of audits, patching, upgrades

# Compliance ≠ Security

*Lessons learned...*

**McAfee**

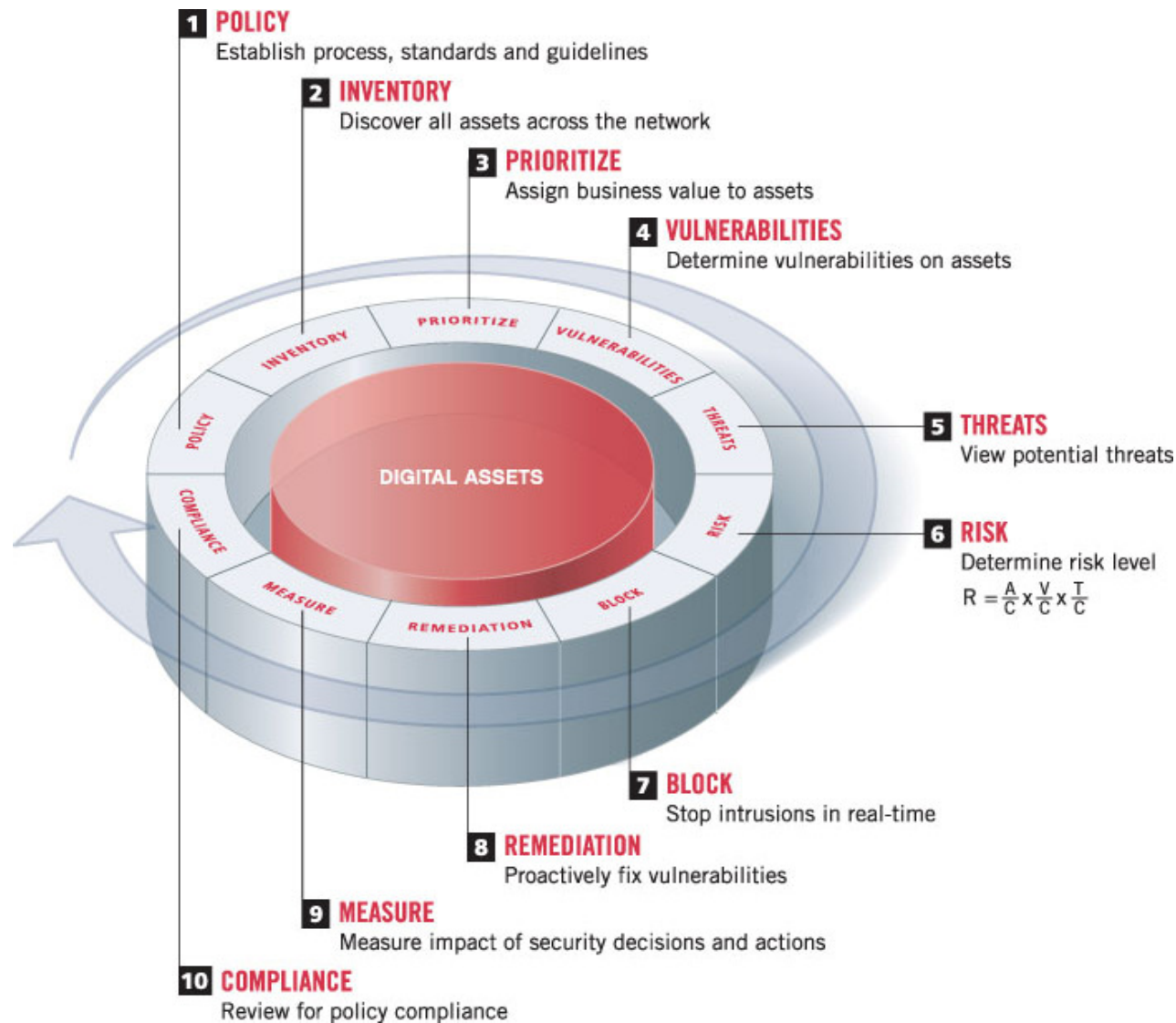




# Managing Security Risk

## Where do we start?

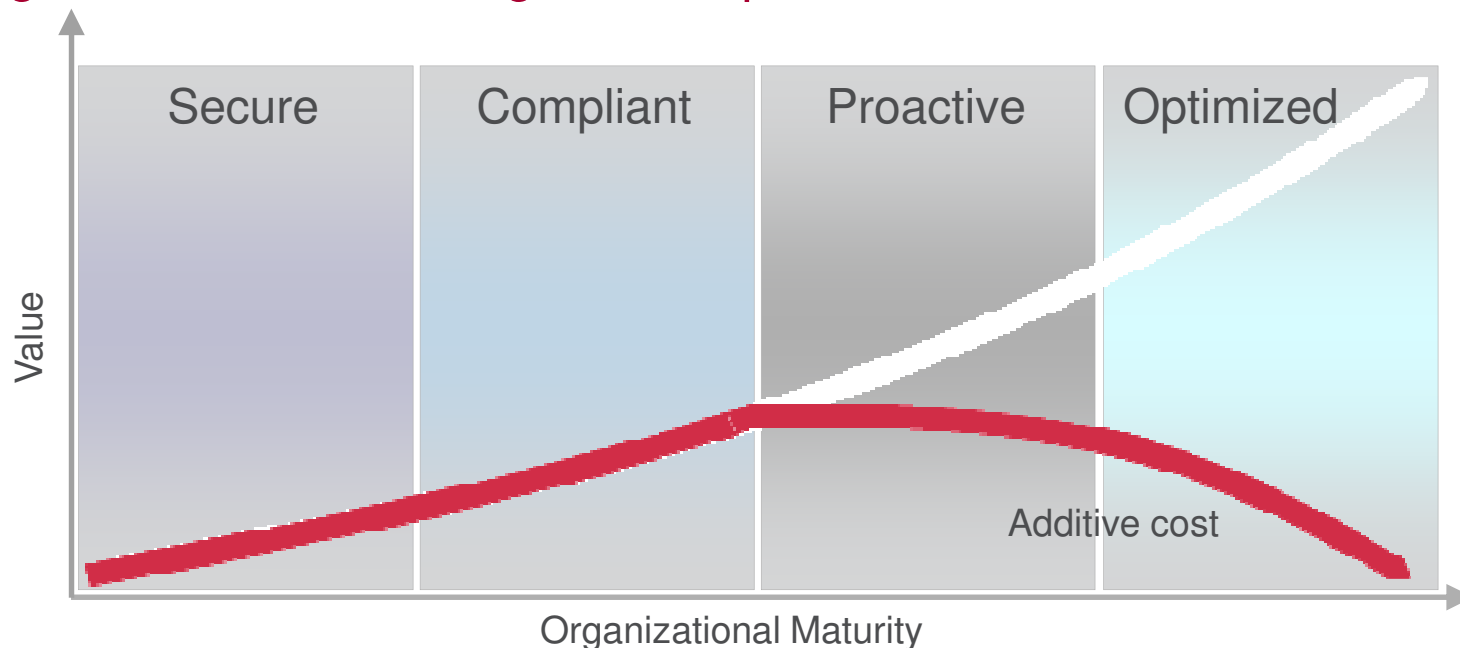
McAfee



## Desired State of IT Audit Maturity – *Optimized*

**McAfee**

The relationship to cost and security and compliance diverge during progression to the managed and optimized states.



- Maturity of process reduces audits from months to days and enables sustainable compliance
- Cost savings occur through reduction of point products and increased automation

# Key Customer Challenges

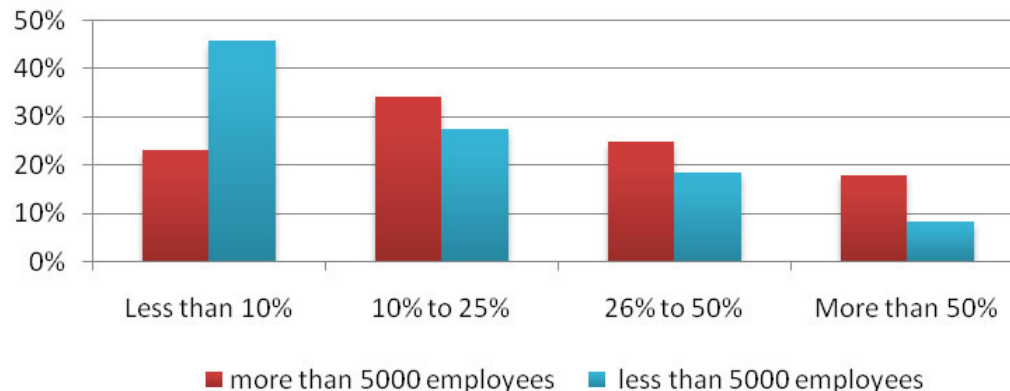
## *“Audit Fatigue” requires Automation*

**McAfee**

*“Majority of IT Audit Controls are Manual”*

**57% of large organizations have automated less than 25% of their controls**

What percentage of controls is automated in your environment?



Collecting accurate, timely data is a protracted effort.

Difficult to ensure integrity of data.

•McAfee- commissioned IT Audit Study: Based on 400 IT audit-related professionals in North America and Europe (ISSA and ISACA). Conducted by the Internet Research Group

# Key Customer Challenges

## *“Patch Panic” creates delays in mitigation*

**McAfee**

*“Anxiety inhibits action”*



### Symptom

- No definitive answer to: “Does the new threat released today apply to us?”

### Statistics

- Microsoft released 78 Security Bulletin items in 2008, with many “out-of-cycle”
- 5443 vulnerabilities added to NVD database in 2008

### Consequences

- Distracts from day-to-day operational workload
- Decreases performance and availability of IT assets
- Exposes a lack of IT leadership and planning

# Managing Security Risk

*How do companies manage it?*

**McAfee**

- **Risk Transfer**

- Contractual transfer to 3rd party or insurance provider.

- **Risk Avoidance**

- The “power button” technique of risk management.

- **Risk Acceptance**

- Cannot eliminate all risk, at some point someone/somewhere must accept what remains.

- **Risk Mitigation**

- Find and apply security countermeasures (people/process/technology)



# Security Metrics

**McAfee**

- **Qualitative**

- Traditional IT audits (EY/PWC/DT) – SAS70/BS7799/ISO17799/ISO27001/ISO27002
- Question/answers
- “Checklist” jockeys/bunnies

- **Quantitative**

- Independently verifiable
- Objective
- Repeatable
- Automatable with technology







Are you spending your  
security dollars *the right*  
*way?*



What kind of return are  
you getting for your  
security dollars?



- **Common Vulnerability Scoring System (0-10)**

- CVSSv2 (2007)
- [www.first.org/cvss](http://www.first.org/cvss)
- Scoring Components (3 major):

- ***Base Metrics***

- *Exploitability Metrics*
      - » Access Vector
      - » Access Complexity
      - » Authentication
    - *Impact Metrics*
      - » Confidentiality Impact
      - » Integrity Impact
      - » Availability Impact

- ***Temporal Metrics***

- Exploitability
    - Remediation Level
    - Report Confidence

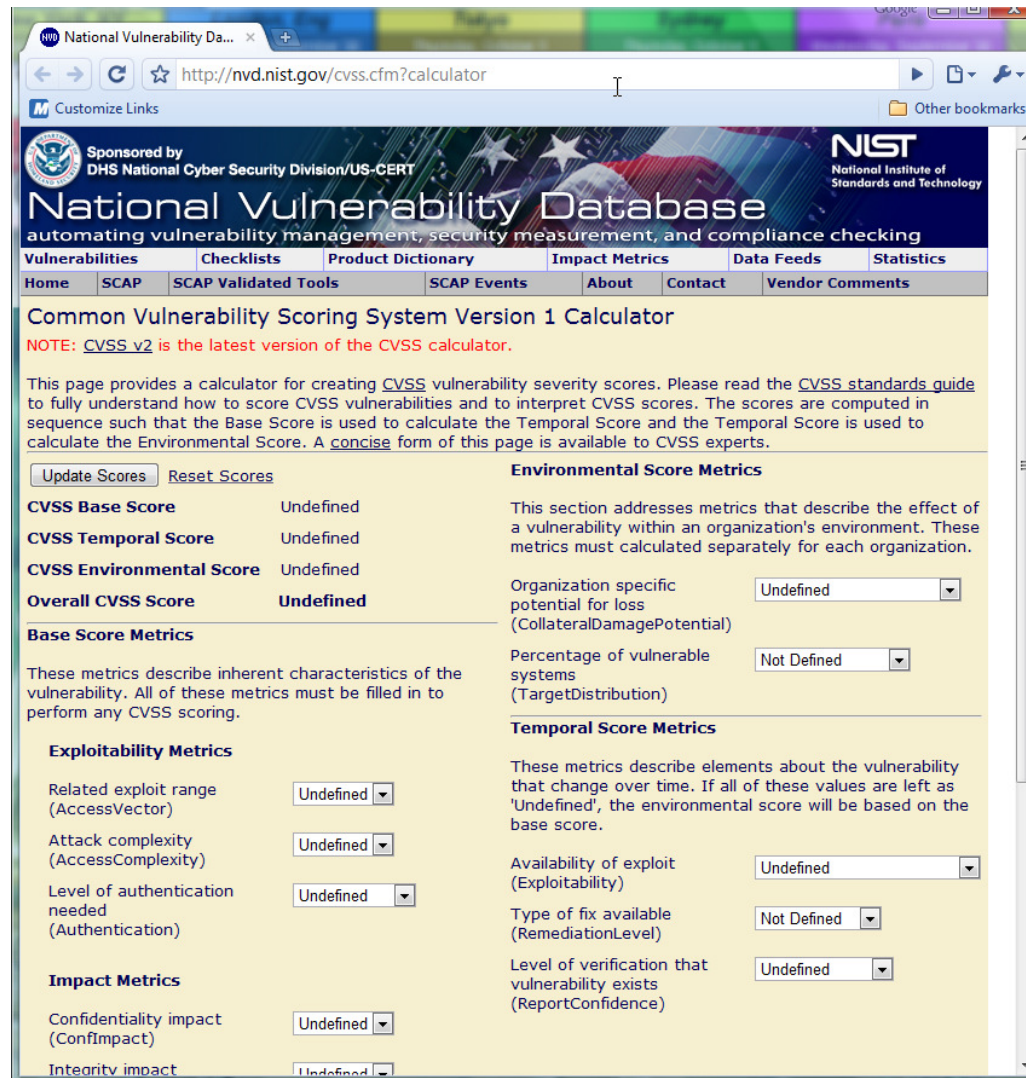
- ***Environmental Metrics***

- Collateral Damage Potential
    - Target Distribution
    - Security Requirements

# FIRST.org (CVSS)

McAfee

- NVD CVSS online calculator



The screenshot shows the National Vulnerability Database (NVD) CVSS calculator interface. The browser address bar displays the URL <http://nvd.nist.gov/cvss.cfm?calculator>. The page header includes the NIST logo and the text "Sponsored by DHS National Cyber Security Division/US-CERT". The main title is "National Vulnerability Database" with the subtitle "automating vulnerability management, security measurement, and compliance checking". Below the title is a navigation menu with links: Vulnerabilities, Checklists, Product Dictionary, Impact Metrics, Data Feeds, and Statistics. The main content area is titled "Common Vulnerability Scoring System Version 1 Calculator". A note states: "NOTE: CVSS v2 is the latest version of the CVSS calculator." The page provides instructions on how to use the calculator and includes a "Concise" form link. The calculator interface is divided into several sections: "Base Score Metrics", "Exploitability Metrics", "Impact Metrics", "Environmental Score Metrics", and "Temporal Score Metrics". Each section contains a list of metrics with corresponding dropdown menus for selection. The "Base Score Metrics" section includes "CVSS Base Score", "CVSS Temporal Score", and "CVSS Environmental Score", all of which are currently set to "Undefined". The "Exploitability Metrics" section includes "Related exploit range (AccessVector)", "Attack complexity (AccessComplexity)", and "Level of authentication needed (Authentication)", all of which are currently set to "Undefined". The "Impact Metrics" section includes "Confidentiality impact (ConfImpact)" and "Integrity impact", both of which are currently set to "Undefined". The "Environmental Score Metrics" section includes "Organization specific potential for loss (CollateralDamagePotential)" and "Percentage of vulnerable systems (TargetDistribution)", both of which are currently set to "Undefined". The "Temporal Score Metrics" section includes "Availability of exploit (Exploitability)", "Type of fix available (RemediationLevel)", and "Level of verification that vulnerability exists (ReportConfidence)", all of which are currently set to "Undefined".

National Vulnerability Database  
Sponsored by  
DHS National Cyber Security Division/US-CERT  
NIST  
National Institute of  
Standards and Technology

Common Vulnerability Scoring System Version 1 Calculator

NOTE: CVSS v2 is the latest version of the CVSS calculator.

This page provides a calculator for creating CVSS vulnerability severity scores. Please read the [CVSS standards guide](#) to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score. A [concise](#) form of this page is available to CVSS experts.

Update Scores Reset Scores

**CVSS Base Score** Undefined  
**CVSS Temporal Score** Undefined  
**CVSS Environmental Score** Undefined  
**Overall CVSS Score** Undefined

**Base Score Metrics**  
These metrics describe inherent characteristics of the vulnerability. All of these metrics must be filled in to perform any CVSS scoring.

**Exploitability Metrics**  
Related exploit range (AccessVector) Undefined  
Attack complexity (AccessComplexity) Undefined  
Level of authentication needed (Authentication) Undefined

**Impact Metrics**  
Confidentiality impact (ConfImpact) Undefined  
Integrity impact Undefined

**Environmental Score Metrics**  
This section addresses metrics that describe the effect of a vulnerability within an organization's environment. These metrics must be calculated separately for each organization.  
Organization specific potential for loss (CollateralDamagePotential) Undefined  
Percentage of vulnerable systems (TargetDistribution) Not Defined

**Temporal Score Metrics**  
These metrics describe elements about the vulnerability that change over time. If all of these values are left as 'Undefined', the environmental score will be based on the base score.  
Availability of exploit (Exploitability) Undefined  
Type of fix available (RemediationLevel) Not Defined  
Level of verification that vulnerability exists (ReportConfidence) Undefined

- **Consensus Metric Definitions v1.0.0 (May 2009)**

- [www.cisecurity.org](http://www.cisecurity.org)
- 20 metric definitions involving:
  - Incident Management
  - Vulnerability Management
  - Patch Management
  - Application Security
  - Configuration Management
  - Financial Metrics
- First realistic security metrics program
- More complex but more complete...



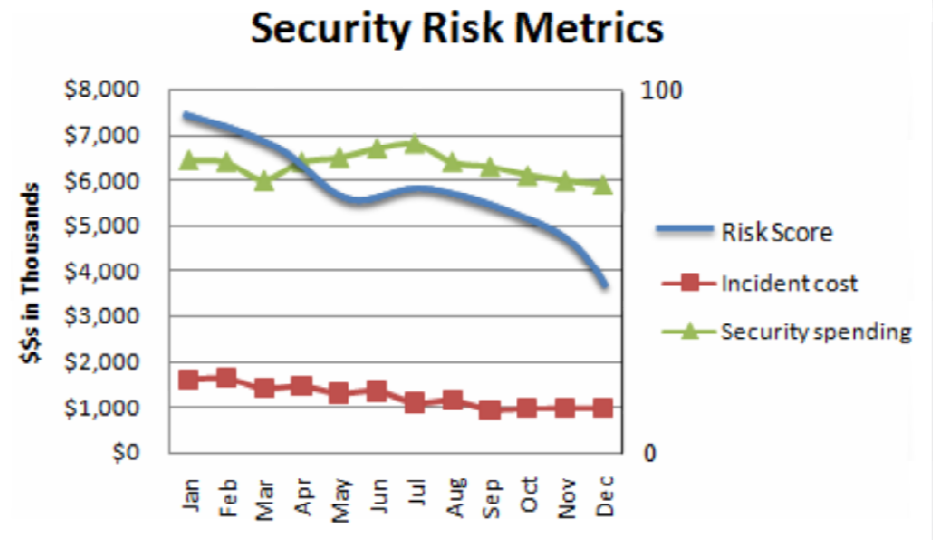
# Quantitative Metrics

*Foster Trust and Credibility...*

McAfee®

## Measure the “Major 3”:

1. Risk Rating (1-100)
  - Attack surface
  - Misused functionality
  - Design flaws
  - WoE
  - User awareness
2. Incident costs (\$\$)
  - Incident expense, loss time quantification, fines/lawsuits associated, notification costs
3. Security expense/spending (\$\$)
  - Operating expenses, Capital expenses



“.. Notification costs per data record are now \$202...”

**Ponemon**  
INSTITUTE

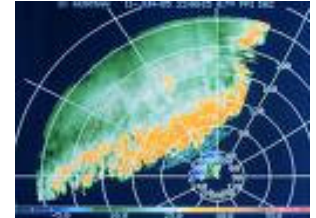


# Quantitative Metrics - Risk Rating

McAfee

- **Attack Surface:**

*How many of you know exactly what assets you have and where you have them?*



*Q: How do you measure attack surface?*

**A: Find and track over time the number of devices on your network:**

- IPv4/IPv6: ICMP, TCP, UDP discover
- IPX/SNA/APPC/AppleTalk
- Query all asset databases, CMDBs, in realtime and on-demand

# Quantitative Metrics - Risk Rating

McAfee

## • Misused Functionality

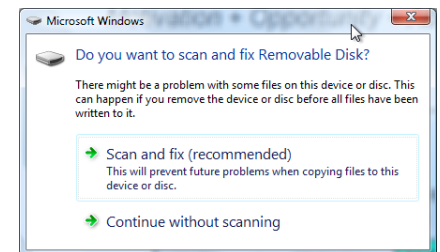


*What configuration settings are present in your environment that contribute to exploitation and malware?*

*Q: How do we measure the number of functions present that can be misused?*

**A: Scan and track over time all your systems for the top 10 configuration weaknesses:**

- Autorun enabled
- File sharing enabled
- Execution permissions on IE Temporary Folders
- Etc...



# Quantitative Metrics - Risk Rating

McAfee

- Design Flaws



*What vulnerabilities are present in your environment that contribute to exploitation and malware?*

*Q: How do we measure the number of vulnerabilities present that can be misused?*

**A: Scan all your systems for at least the following:**

- Microsoft Security Bulletins
- SANS Top 20 or similar
- OWASP Top 10 and/or CWE 25 (Web)



MITRE

# Quantitative Metrics - Risk Rating

McAfee

- Window of Exposure (WoE)



*How quickly does IT fix the problems that security finds?*

*Q: How do we measure your IT staff's ability to patch and remediate the misused functionality and design flaws found?*

**A: Measure it with technology:**

- Vulnerability Management program
- Patch Management program
- Configuration Management program
- Find the mis-configurations and vulnerabilities and measure how quickly they are remediated.

- **User Awareness**

*How educated are your users on general security hygiene?*

*Q: How do we measure your user's preventative awareness?*

**A: Ask them (questionnaire - ideally at login):**

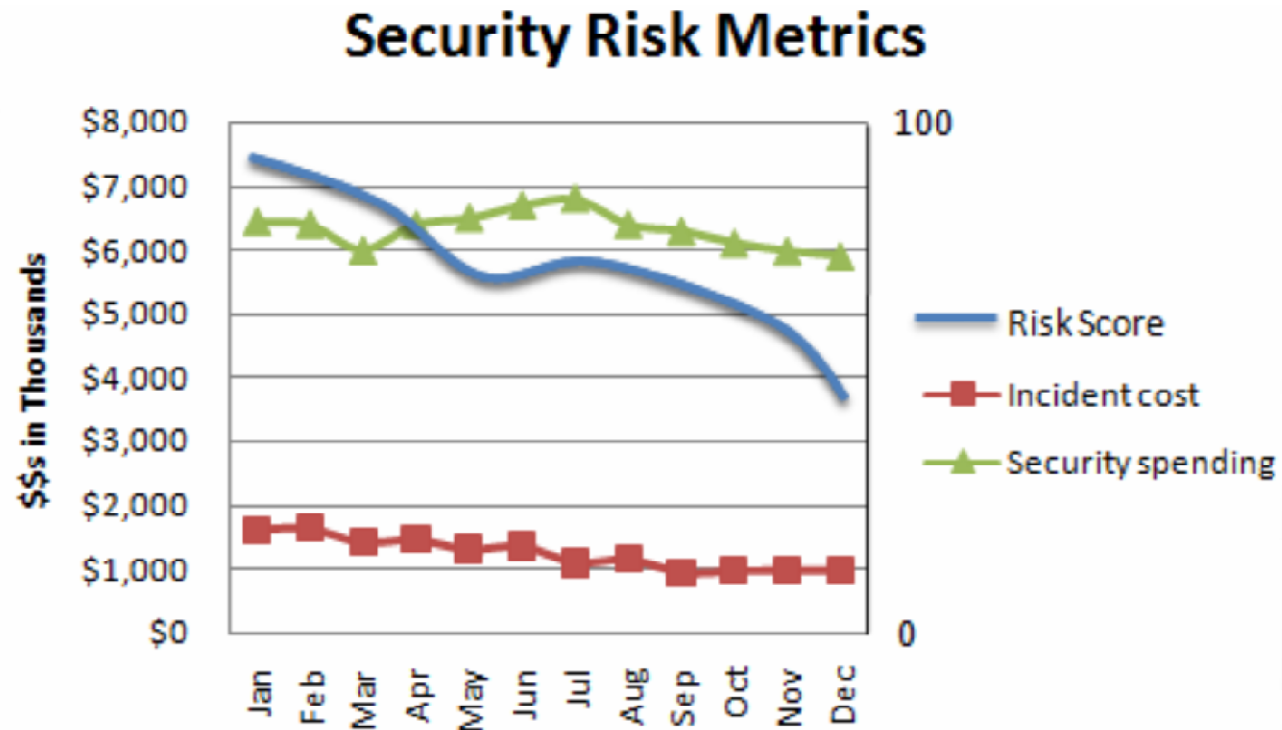
- Pick 5 to 10 questions about general user decision making skills:

1. If you receive an attachment or a web link from someone you don't know, do you open it?
2. If you are given a USB key, do you plug it into your computer without scanning it?
3. Do you go to websites you do not know are safe?
4. Etc...



# Quantitative Metrics - Overall

McAfee®





# Design Flaws – Return on Investment

## SDLC



- Microsoft's Software Development Lifecycle (SDL)



- Reduce the number of vulnerabilities
- Reduce the overall development costs
- NIST, May 2002 – eliminating vulnerabilities in design can cost 30x less than fixing them after release.
- Microsoft ROI whitepaper: <http://go.microsoft.com/?linkid=9684360>

# Behavioral Analysis

*Applied to Security...*

**McAfee**

*Motivation + Opportunity + Ability = **Potential***

## **Motivation**

- Value of data available
- Laxed or non
- Ease or diffic

## **Opportunity**

- # of interconnected devices
- # of vulnerabilities
- # of functions available to misuse
- Sophistication of users/admins
- # of tools available
- # of domain registrations
- # of websites accessible

## **Ability**

- Knowledge level of the bad guys
- Criminal mentality
- Information publicly available

## Conclusion



- Threats and events continue to increase
- Stay abreast with current world events
- Understand the current economic climate
- Understand your organization's needs
- Measure EVERYTHING!

Thank you!

[stuart\\_mcclure@mcafee.com](mailto:stuart_mcclure@mcafee.com)

949-297-5585